

1 CUAUHTEMOC ORTEGA (Bar No. 257443)  
2 Federal Public Defender  
3 ANNE O'TOOLE (Bar No. 340469)  
(E-Mail: annie\_otoole@fd.org)  
4 CLAIRE KENNEDY (Bar No. 333632)  
(E-Mail: claire\_kennedy@fd.org)  
5 Deputy Federal Public Defenders  
6 321 East 2nd Street  
7 Los Angeles, California 90012-4202  
Telephone: (213) 894-2854  
Facsimile: (213) 894-0081

8  
9 Attorneys for Defendant  
10 HERBERT REDHOLTZ  
11

12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

**UNITED STATES DISTRICT COURT**  
**CENTRAL DISTRICT OF CALIFORNIA**  
**WESTERN DIVISION**

UNITED STATES OF AMERICA,

Plaintiff,

v.

HERBERT REDHOLTZ,

Defendant.

Case No. 2:22-cr-433-MCS

**HERBERT REDHOLTZ'S  
STATUS REPORT**

Herbert Redholtz, by and through his attorneys of record, Deputy Federal Public Defenders, Anne O'Toole and Claire Kennedy, hereby files the enclosed status report, as requested by the Court during the March 4, 2024 suppression hearing. The parties have not reached stipulation or agreement as to the factual record and therefore are filing separate positions.

Respectfully submitted,

CUAUHTEMOC ORTEGA  
Federal Public Defender

DATED: March 22, 2024

By /s/ Anne O'Toole

ANNE O'TOOLE  
CLAIRE KENNEDY  
Deputy Federal Public Defenders  
Attorneys for HERBERT REDHOLTZ

1       At the March 4, 2024 suppression hearing, the Court identified three factual  
 2 issues important to its ruling on Mr. Redholtz’s motions to suppress: (1) the date that  
 3 Microsoft returned email data to Homeland Security Investigations (“HSI”) (*i.e.*  
 4 whether it was March 19, 2015, two days after the warrant was served and within the  
 5 10 days that Microsoft was required to respond to the warrant (defense position) or  
 6 May 21, 2015, two months after the time period within which Microsoft was required  
 7 to respond to the warrant (government position)); (2) the date range of the data that  
 8 Agent Sampson’s bookmarks covered (*i.e.* did any of the bookmarked data pre-date  
 9 October 17, 2014—the starting point of the warrant’s time period?); and (3) whether  
 10 Agent Baker’s (or Agent Salaam’s or another agent’s) review in 2019 or 2020 of the  
 11 original case agent’s bookmarks implicated the email data itself, such that it constituted  
 12 a search.<sup>1</sup>

13       The Court requested that the parties endeavor to ascertain additional information,  
 14 particularly with respect to #1. As of this writing, however, all three issues remain live.  
 15 On March 20, 2024, the government provided some very limited discovery to the  
 16 defense, without necessary context to interpret that discovery. On March 21, the  
 17 defense sent an additional discovery request and re-iterated certain prior requests,  
 18 which may yet lead to resolution of some of the outstanding issues. Specifically, the  
 19

---

20       <sup>1</sup> As the Court acknowledged during the suppression hearing, the portion of the  
 21 affidavit in support of the June 2020 warrant that discussed the NCMEC CyberTip and  
 22 Agent Sampson’s review of the email and image associated with the CyberTip did not  
 23 contain language regarding hash values such that it might be able to support a finding  
 24 of probable cause under *United States v. Wilson*, 13 F.4th 961 (9th Cir. 2021).  
 25 Reference to the magistrate case number for the previously-issued warrant does not  
 26 suffice to incorporate the earlier warrant’s discussion of hash values. *See United States*  
 27 *v. Anderson*, 453 F.2d 174, 175 (9th Cir. 1971) (“all data necessary to show probable  
 28 cause for the issuance of a search warrant must be contained within the four corners of  
 a written affidavit given under oath”). The only remaining information to support  
 probable cause for the June 2020 warrant is therefore: (1) a statement that Mr. Redholtz  
 made that he used the Hotmail account for a number of years, and (2) a discussion of  
 the bookmarks that Agent Sampson made of the Microsoft data.

1 defense requested information about and inspection of the bookmarks by March 28. On  
2 March 22, 2024, the government produced some additional information that supports  
3 the defense's position that data responsive to the warrant was produced on March 19,  
4 2015, but did not provide the full scope of information requested by the defense.  
5 Accordingly, the defense would propose submitting a further status update on Friday,  
6 March 29, 2024 on the key issues outlined above. If the issues still have not been  
7 resolved at that point, the defense would request that the Court hold an evidentiary  
8 hearing at which Agent Sampson, Agent Baker, Agent Salaam, and/or any other agent  
9 involved in creating and/or reviewing the Microsoft data or bookmarks would testify.

10 **Microsoft's return of email data to HSI**

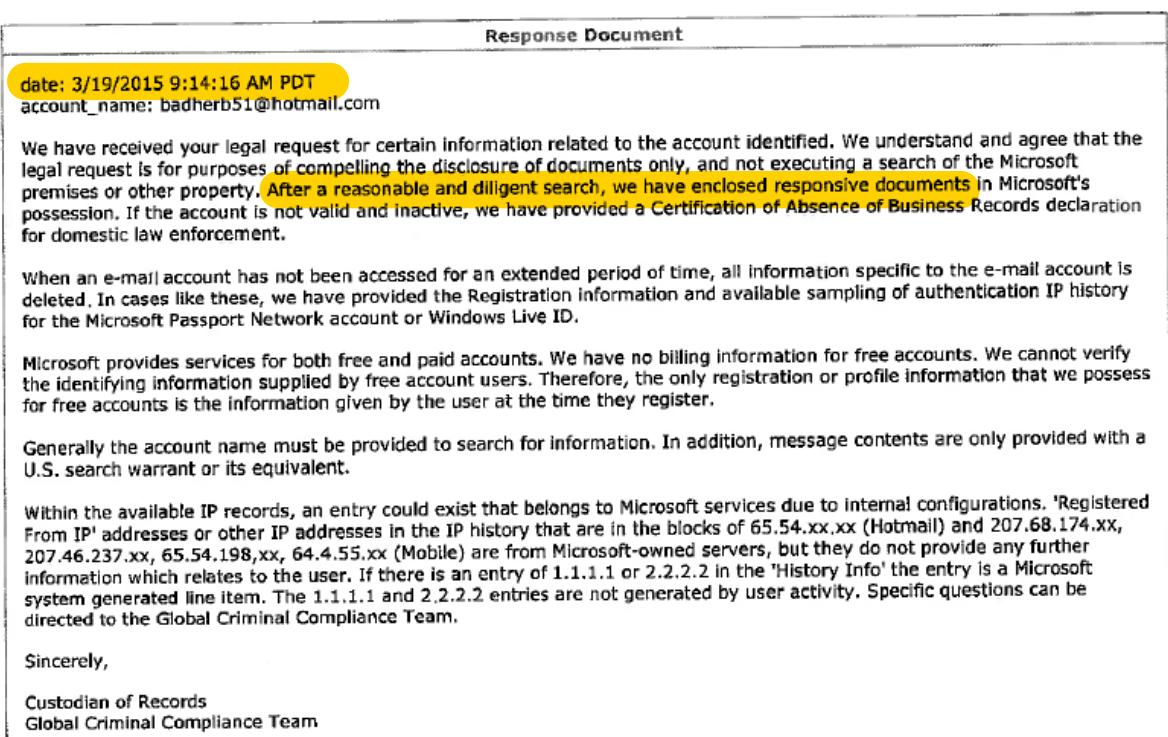
11 The first issue for the Court's consideration is the date that Microsoft returned  
12 email data to HSI. This date matters because if the defense is correct that the data was  
13 returned on March 19, 2015, then Agent Sampson's reviews (and bookmarks) of that  
14 data were outside of the scope of the warrant, which required her to complete her  
15 review within 60 days of receipt of the data. Accordingly, the discussion of the  
16 bookmarks in the later June 2020 warrant should be excised from the probable cause  
17 determination for that warrant. With respect to this issue, the government initially  
18 produced on Wednesday, March 20, 2024 three communications not previously  
19 produced to Mr. Redholtz in discovery.

20 First was an email dated March 15, 2024 from Microsoft to the government's  
21 case agent stating that Microsoft no longer has any data reflecting when Microsoft  
22 transmitted or sent the Microsoft email data to HSI. Mr. Redholtz also obtained a  
23 subpoena from the Court to Microsoft for this information, and on Friday, March 22,  
24 2024, Microsoft emailed defense counsel and stated that no data was found in response  
25 to the subpoena. *See Ex. A.*

26 The government also produced two emails dated May 22, 2015 (not May 21,  
27 2015—its earlier position) from Microsoft to Agent Sampson with URLs for secure file  
28 transfers, and access keys for those URLs, which Agent Sampson was apparently able

1 to locate in her email archive earlier this week. The government did not, however,  
 2 produce any context around those emails. For example, the government did not produce  
 3 emails from just before or after that date or any emails from around the critical March  
 4 17-19, 2015 time period, which would shed more light on the defense's position. The  
 5 government also did not produce any information reflecting whether these emails from  
 6 Microsoft were in response to any emails sent by Agent Sampson to Microsoft. It is not  
 7 clear whether the May 22, 2015 emails were actually a re-production, or second  
 8 transmittal, of data, rather than the first. Accordingly, defense counsel sent the  
 9 government a supplemental discovery request for all email communications between  
 10 Agent Sampson and Microsoft between March 12, 2015 (which is tied to Microsoft's  
 11 response to an earlier 2703 order) and May 22, 2015. *See* Ex. B.

12 The government also continues to point to a handwritten case chronology written  
 13 by Agent Sampson to support its theory that Microsoft's first response to the March 17,  
 14 2015 warrant occurred on May 22, 2015. But this case chronology does not account for  
 15 the fact that Microsoft clearly sent a response to HSI on March 19, 2015, which is not  
 16 reflected on that chronology. *See* Dkt. 56 Ex. C (pasted below):

17  Response Document

18 date: 3/19/2015 9:14:16 AM PDT  
 account\_name: badherb51@hotmail.com

19 We have received your legal request for certain information related to the account identified. We understand and agree that the  
 legal request is for purposes of compelling the disclosure of documents only, and not executing a search of the Microsoft  
 premises or other property. After a reasonable and diligent search, we have enclosed responsive documents in Microsoft's  
 possession. If the account is not valid and inactive, we have provided a Certification of Absence of Business Records declaration  
 for domestic law enforcement.

20 When an e-mail account has not been accessed for an extended period of time, all information specific to the e-mail account is  
 deleted. In cases like these, we have provided the Registration information and available sampling of authentication IP history  
 for the Microsoft Passport Network account or Windows Live ID.

21 Microsoft provides services for both free and paid accounts. We have no billing information for free accounts. We cannot verify  
 the identifying information supplied by free account users. Therefore, the only registration or profile information that we possess  
 for free accounts is the information given by the user at the time they register.

22 Generally the account name must be provided to search for information. In addition, message contents are only provided with a  
 U.S. search warrant or its equivalent.

23 Within the available IP records, an entry could exist that belongs to Microsoft services due to internal configurations. 'Registered  
 From IP' addresses or other IP addresses in the IP history that are in the blocks of 65.54.xx.xx (Hotmail) and 207.68.174.xx,  
 207.46.237.xx, 65.54.198.xx, 64.4.55.xx (Mobile) are from Microsoft-owned servers, but they do not provide any further  
 information which relates to the user. If there is an entry of 1.1.1.1 or 2.2.2.2 in the 'History Info' the entry is a Microsoft  
 system generated line item. The 1.1.1.1 and 2.2.2.2 entries are not generated by user activity. Specific questions can be  
 directed to the Global Criminal Compliance Team.

24 Sincerely,

25 Custodian of Records  
 26 Global Criminal Compliance Team

1       Moreover, evidence produced by the government just today supports the  
2 defense's position that Microsoft must have responded to the warrant on March 19,  
3 2015. In its opposition and at the hearing, the government incorrectly claimed that the  
4 March 19, 2015 transmittal notice (pasted above) was Microsoft responding to an 18  
5 U.S.C § 2703(d) order—not Microsoft responding to the warrant that was served just  
6 two days prior. *See* Dkt. 61 at 4 (government's opposition claiming that "Microsoft  
7 produced data responsive to this order on March 19, 2015" and stating that the defense  
8 "mischaracterize[d] this data response from Microsoft as being produced in response to  
9 the subsequent warrant for email content."). But today, the government produced  
10 evidence revealing that its position is plainly incorrect. Two emails produced by the  
11 government confirm that Microsoft responded to the 18 U.S.C. § 2703(d) order on  
12 March 12, 2015, just as the defense stated during the suppression hearing. *See* Ex. C  
13 (copies of Agent Sampson's emails showing that Microsoft responded to the § 2703(d)  
14 order on March 12, 2015). Clearly, the March 19, 2015 transmittal notice was not in  
15 response to the § 2703(d) order, and instead, clearly represents Microsoft's response to  
16 the search warrant.

17       March 19, 2015 also makes logical sense as Microsoft's production date, since it  
18 was just two days after Microsoft received the warrant and occurred during the 10-day  
19 time period within which Microsoft was ordered by the warrant to provide the  
20 requested information. Without further information, the defense does not accept the  
21 government's cherry-picked production of two emails that are seemingly helpful to its  
22 own argument. Especially because it's clear that Agent Sampson had other email  
23 communications with Microsoft that were not retrieved from her email archives in  
24 preparation for this status report (namely, the transmittal notice pasted above).

25       Even if further information somehow reveals that the government is correct that  
26 Microsoft first produced responsive data to the March 17, 2015 warrant on May 22,  
27 2015, that production of information would still have been outside the scope of the  
28 warrant. The March 17, 2015 warrant ordered Microsoft to deliver the information set

1 forth in the warrant “*within 10 days of the service of this warrant.*” Dkt. 56 Ex. A at  
 2 USAO\_000294-95 ¶ 12 (emphasis added). It is undisputed that Agent Sampson faxed  
 3 the warrant to Microsoft on March 17, 2015. Therefore, Microsoft should have returned  
 4 responsive data by March 27, 2015 at the latest. If Microsoft’s return of the data was  
 5 untimely under the terms of the warrant, it should not automatically toll the  
 6 government’s review deadline. Consider if Microsoft responded to a warrant 10 years  
 7 late. The government should not be able to review the warrant returns 10 years and 60  
 8 days after it obtained the warrant from the Court. If Agent Sampson really did not  
 9 receive any Microsoft data for the Hotmail account until May 22, 2015, she should not  
 10 have assumed she had authority to review that data which was untimely returned.<sup>2</sup>

11 **The date range of the bookmarks**

12 Microsoft produced, and HSI seized, the entire contents of the Microsoft account,  
 13 rather than the data from the time period set by the warrant: “after October 17, 2014.”  
 14 Dkt. 56 Ex. A at USAO\_000293-94 ¶ 11(a). At the suppression hearing, the Court  
 15 asked if the parties knew whether the bookmarks created by Agent Sampson  
 16 corresponded with the correct time period of the warrant (after October 17, 2014), or if  
 17 they also covered any data that predated that time period. The reason why this matters  
 18 is because if the bookmarks implicated any data that was seized outside of the scope of  
 19 the warrant, the description of the bookmarks should also be excised from the Court’s  
 20 consideration of probable cause for the June 2020 warrant.

21 The answer to this question is still unclear, though Mr. Redholtz first requested  
 22 “the opportunity to inspect the bookmarks and underlying bookmarked files” over a  
 23 year ago. *See* Ex. D (March 21, 2023 discovery request letter). Defense counsel has  
 24 reiterated this request several times since then, but has not been given any further  
 25

---

26       <sup>2</sup> The defense’s secure data reviews reflected that the last date of email produced  
 27 by Microsoft was from March 17, 2015. This aligns with Microsoft receiving a warrant  
 28 on March 17, 2015, promptly preserving the data requested, and submitting the data to  
 HSI within the 10 days required by the warrant.

1 information about the bookmarks or the opportunity to inspect them, despite  
2 completing three secure discovery reviews—one at the United States Attorney’s Office  
3 and two at HSI’s office in Long Beach. On March 21, 2024, Mr. Redholtz re-iterated  
4 his request for inspection of the bookmarks, which would shed light on the date range  
5 that they cover.

6 **Whether review of the bookmarks implicated the underlying data**

7 Finally, it remains an open question what Agent Baker, Agent Salaam, or another  
8 agent actually reviewed in 2019 or 2020 when he or they determined that “SA Sampson  
9 had not completed her review” of the Microsoft data, and that she had bookmarked  
10 1,195 items as potential child abuse material and 1,054 items as potential child-  
11 exploitive material, while leaving 250,321 items uncategorized. Dkt. 56 Ex. D  
12 USAO\_000362 ¶ 28. This issue matters because if a government agent actually  
13 accessed the Microsoft data to draw these conclusions, then that would have been a  
14 warrantless search, and so the discussion of the bookmarks should again be excised  
15 from the June 2020 warrant as the Court determines whether that warrant was  
16 supported by probable cause.

17 At the motions hearing, the government represented that Agent Baker’s review of  
18 the bookmarks did not require him to review any of the underlying data. However, the  
19 government did not base that assertion on any factual evidence, since Agent Baker was  
20 not present at the hearing and it appears that the government has never actually done its  
21 own independent review of the underlying data or bookmarks. Moreover, as defense  
22 digital forensics expert Jake Gibson explained: “In order to draw these specific  
23 conclusions, Agent Baker or a colleague must have reviewed, in a forensic software  
24 program, the underlying data that Microsoft had produced in response to the March  
25 2015 warrant and Agent Sampson’s work product.” Dkt. 56 Gibson Decl. ¶ 13. The  
26 government shed no light on this issue beyond a vague, one-sentence declaration from  
27 Agent Baker stating: “Prior to obtaining a search warrant on June 3, 2020, to search  
28 defendant’s Microsoft email data (Case No. 20-MJ-2510), I had not reviewed the

1 content of the Microsoft email data, including the date ranges of that email data.” Dkt.  
2 61 Baker Decl. ¶ 2.

3 On March 21, 2024, the defense therefore re-iterated its prior requests for  
4 inspection of the bookmarks and requested further information about who viewed the  
5 bookmarks, when, and how, as well as screenshots of what the person who reviewed  
6 the bookmarks would have seen. Ex. B. In other words, if reviewing the bookmarks  
7 does not also require viewing the underlying data, then the government should be able  
8 to provide such a screenshot. If the government does not provide the requested  
9 information, then the defense believes an evidentiary hearing is necessary to learn more  
10 from the agent who actually reviewed the bookmarks.

11  
12 Respectfully submitted,

13 CUAUHTEMOC ORTEGA  
14 Federal Public Defender

15 DATED: March 22, 2024

16 By /s/ Anne O'Toole

17 ANNE O'TOOLE  
18 CLAIRE KENNEDY  
19 Deputy Federal Public Defenders  
20 Attorneys for HERBERT REDHOLTZ

21  
22  
23  
24  
25  
26  
27  
28